SECUREDATA, Inc.
SecureDrive BT

FIPS 140-2 Non-Proprietary Security Policy
Version 1.4

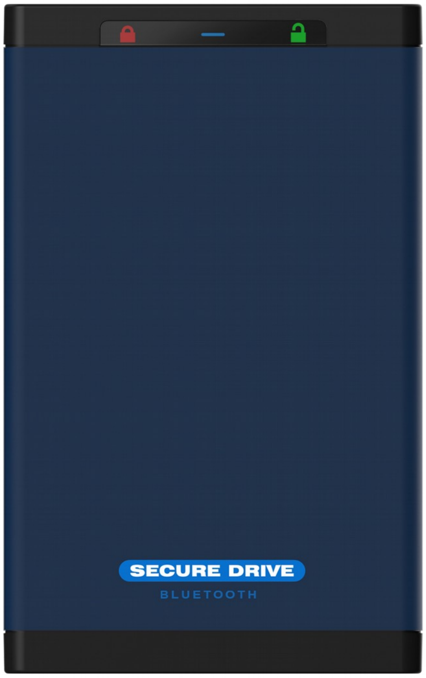

Table of Contents

List of Tables

List of Figures

1 Cryptographic Module Specification

1.1 Overview

The SECUREDATA, Inc. SecureDrive-BT is a multi-chip, stand-alone, cryptographic module that provides hardware-encrypted storage of user data with a USB 3.0 interface. Access to encrypted data is authenticated via the Bluetooth interface. User data is protected by 256-bit XTS-AES encryption that secures sensitive information from unauthorized disclosure in the event that the module is lost or stolen. The custom electronics within the module are encapsulated within an opaque, production grade epoxy. The module's enclosure defines the cryptographic boundary.

The data encryption key (DEK) and other critical security parameters (CSPs) are generated by a NIST approved DRBG[1] within the module when it is first used. The seed for the DRBG is also produced within the module from a hardware-based, entropy generator.

The user interface for the module is three (3) status-indicators LEDs. The LEDs are each a different color, red, green, and blue.

[1] SP 800-90Ar1 – Recommendation for Random Number Generation Using Deterministic Random Bit Generators. NIST. (June 2015).

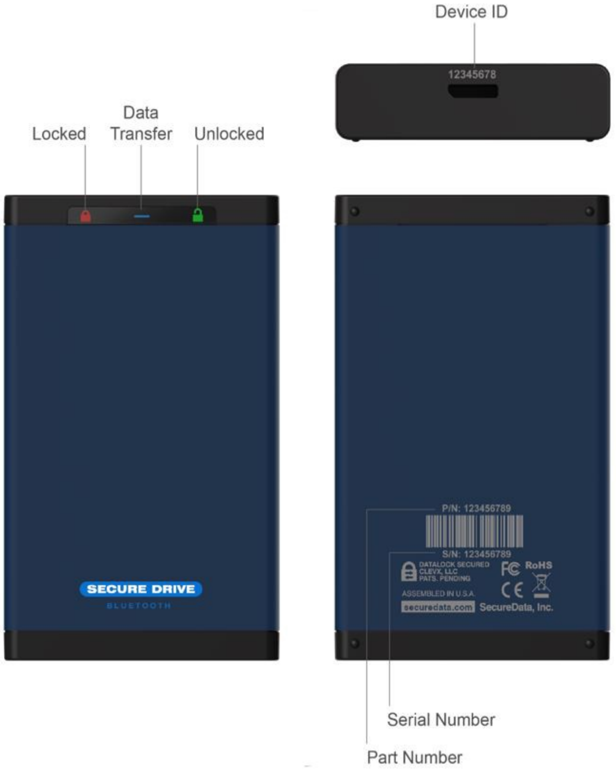

Figure 1: SecureDrive BT

Hardware Part Numbers	**Firmware Versions** (implemented on all hardware versions)
SD-BT-12-BU-1TB SD-BT-12-BU-2TB SD-BT-20-BU-1TB SD-BT-20-BU-2TB SD-BT-20-BU-4TB SD-BT-20-BU-5TB SD-BT-12-BU-250GB-SSD SD-BT-12-BU-500GB-SSD SD-BT-12-BU-1TB-SSD SD-BT-12-BU-2TB-SSD SD-BT-12-BU-4TB-SSD SD-BT-12-BU-8TB-SSD	Each module has one each of Firmware A and Firmware B. *Firmware A* CLEVX_3637E_USB_V0313 or CLEVX_3637E_USB_V0314 (no security relevant differences) *Firmware B* CLEVX_SATA-BT_v2.3

Table 1: Module Hardware and Firmware Versions

1.2 FIPS Security Level

The module meets the overall requirements for FIPS 140-2[2] Level 3.

FIPS Area	FIPS Security Requirement	Level
1	Cryptographic Module Specification	3
2	Module Ports and Interfaces	3
3	Rôles, Services, and Authentication	3
4	Finite State Model	3
5	Physical Security	3
6	Operational Environment	*n/a*
7	Cryptographic Key Management	3
8	EMI/EMC	3
9	Self-Tests	3
10	Design Assurance	3
11	Mitigation of Other Attacks	*n/a*

Table 2: FIPS Security Level

[2] *FIPS 140-2 – Security Requirements for Cryptographic Modules*. NIST. (December 2002).

1.3 Mode of Operation

The module operates only in a FIPS approved mode. Approved mode is indicated by the three status-indicator LEDs illuminating one at a time, green, blue, and then red when the module is powered on. This indication means that firmware integrity checks and KATs have successfully passed.

To meet the requirements for FIPS 140-2 Level 3, the module enforces the following security rules:

- The cryptographic module provides two distinct operator rôles: User and Cryptographic Officer (CO).
- The cryptographic module provides identity-based authentication.
- When the module has not been placed in a valid rôle or is in an error state, the operator shall not have access to any cryptographic service.
- The operator is capable of commanding the module to perform self-tests at any time by cycling the power.
- Data output is inhibited during self-test, zeroization, key generation, and authentication.
- No CSPs are output from the module in any form.
- Each unique AES GCM/IV pair is used for one and only one secure communication session.
- Each secure communication session is established between exactly two entities.
- The module cannot establish a secure communication session with another, identical module.

2 Module Ports and Interfaces

The cryptographic module exposes the following physical ports and logical interfaces:

Physical Port	Logical Interface	Description
USB Data	Data input Data output Control input Status output	The USB Data port connects the module to the host computer. It is used to exchange decrypted user data as well as control and status information for the USB protocol. When the drive is locked the USB interface is disabled.
Bluetooth	Control input Status output Data input Data output	User and CO Password received and module status information transmitted via the Bluetooth port.
Red, green and blue LEDs	Status output	Refer to Table 4 for details.
USB Power	External power	The USB VBUS (+5VDC) powers the module and embedded storage component.

Table 3: Module Ports and Interfaces

LED Behavior[3]	Module State	Status Description
LEDs illuminate one at a time, green, blue, and then red. Red remains lit.	Connected to USB power	Module powered-on with all LEDs operational. Firmware integrity tests and KATs have passed.
LEDs illuminate continuously in circling pattern, red then green then blue.	Failed	Module in error state.
Red LED illuminated	Locked	Module locked. User data secure.
Green LED illuminated	Unlocked	Module unlocked. DEK is unwrapped. USB interface with host has not enumerated with the host computer.
Green and blue LED illuminated	Connected	Module unlocked and connected to host computer.
Green LED illuminated. Blue LED blinking	Connected	Module unlocked and connected to host computer. There is an active data transfer with host computer.

Table 4: LED Status Indications

To verify that the module is in good working order when it is first powered-on, observe that the three status-indicator LEDs illuminate one at a time green, then blue, and then red. Red remains lit indicating that the module is locked.

[3] Because the module is powered from USB, the LED indicators are valid only when when the module is connected to a USB port.

3 Rôles, Services, Authentication, and Identification

3.1 Rôles and Identification

The module implements level 3, identity-based authentication with two distinct rôles.

Identity	Identification	Authentication Data	Description
User[4]	User chooses ASCII value '1' for User identification.	7-15 character Password	User has full access to all User services.
CO	CO chooses ASCII value '0' for CO identification.	7-15 character Password	CO has full access to all CO services.

Table 5: Module Rôles

3.2 Module Initialization

A new module comes from the factory initialized with a default User Password of '11223344'. No CO Password is defined for a factory initialized module. In this configuration, the module is ready for operation in a FIPS approved mode.

If the module is zeroized, there will be neither a User Password nor a CO Password defined and there will be no DEK. The module must be initialized before it will operate in an approved mode. From this state, either a User or a CO Password may be defined first.

[4] In the case where the User password is defined but no CO password is defined, the User identity behaves as a combined User/CO identity.

3.3 Services

Identity	Service	CSP Access
CO	Set CO Password	Read and Write Change CO Password, CO salt, and CO KEK. Create DEK using CTR-DRBG state (seed, V, key) if one is not defined.
	Set User Password	Read and Write Change User Password, User salt, and User KEK.
	Zeroize User Password	Zeroize Zeroize User salt and User KEK.
	Erase private partition data	Read and Write Change CO salt and CO KEK. Create DEK using CTR-DRBG state (seed, V, key). Zeroize Zeroize User salt and KEK.
	Open private partition for read/write access to user data	Read Read CO salt and CO KEK. Decrypt DEK.
	Lock private partition to prevent read/ write access to user data	Zeroize Zeroize DEK in RAM.
	Read or write private partition with user data	Read Use DEK to encrypt and decrypt user data.
	Configure idle timeout lock	None
	Configure Remote Management	None
	Change nickname	None
	Configure Step-Away lock	None
User	Set CO Password when none exists	Read and Write Change CO Password, CO salt, and CO KEK.
	Set User Password	Read and Write Change User Password, User salt, and User KEK. Create DEK using CTR-DRBG state (seed, V, key) if one is not defined.
	Open private partition for read/write access to user data	Read Read CO salt and CO KEK. Decrypt DEK.
	Lock private partition to prevent read/ write access to user data	Zeroize Zeroize DEK in RAM.
	Read or write private partition with user data	Read Use DEK to encrypt and decrypt user data.
	Configure idle timeout lock	None
	Change nickname	None
	Configure Step-Away lock	None

Identity	Service	CSP Access
Unauthenticated	Show locked/unlocked status	None
	Show whether or not drive is initialized	Read Verify validity of either User salt or CO salt.
	Show whether or not User Password is defined	Read Verify validity of User salt.
	Show whether or not CO/Password is defined	Read Verify validity of CO salt.
	Run self-tests	None
	Factory reset (zeroize) module and erase private partition data	Zeroize Zeroize all CSPs.
	Query firmware version	None
	Authentication	Read and Write Create and read ECC-CDH Private Key, Session Master Secret, AES-GCM Key/IV

Table 6: Services Available in FIPS Approved Mode

3.4 Authentication

The Crypto Officer and User rôles authenticate via the Bluetooth interface. The module does not output CO or User authentication data outside of the cryptographic boundary. Communication via the Bluetooth interface is protected by encryption. Messages are encrypted and authentication with AES-GCM (Cert. #5397). Cryptographic keys are established per SP 800-56Ar2 scheme C(0s,2e,ECC_CDH), conforming to FIPS 186-4 (ECDSA Cert. #1428) and CVL (Cert. #1857), and derived using KBKDF (Cert. #201) in Counter Mode, which relies on AES-CMAC (Cert. #5366) and HMAC-SHA-1 (Cert. #3554) per SP 800-108.

The Password, from either the User or the CO, is an input to PBKDFv2 that produces the Key Encryption Key (KEK) for that rôle. The KEK is used by the Synthetic Initialization Vector[5] (SIV) algorithm to encrypt or wrap the DEK. SIV is constructed using AES CTR (Cert. #5366) and AES CMAC (Cert. #5366). Decrypting (sometimes called unwrapping) an encrypted DEK requires the same Password that was given to PBKDFv2 when the DEK was encrypted.

The authentication strength for the module is determined by the Password. The Password is composed of a sequence of UTF-8 characters selected by the User or CO. The minimum Password length is seven (7) bytes. The maximum Password length is 15 bytes. The probability of a successful, random guess of a minimum length Password is approximately $(10+26+26+20^{6})^{-7}$ or 1 chance in 10^{13} which is much smaller than 1 chance in 10,000,000[7].

The module protects against brute-force attempts to guess a rôle's Password by permitting no more than ten (10) consecutive incorrect guesses before locking out that rôle. Incorrect Password attempts are counted independently for each rôle. The probability of an attacker correctly guessing a Password is much smaller than 10^{-6} or 1 chance in 1,000,000.

[5] Harkins, D. *Synthetic Initialization Vector (SIV) Authenticated Encryption Using the Advanced Encryption Standard (AES)*. IETF. (October 2008)

[6] The explicitly included characters are ten digits 0-9, upper and lower case ASCII letters A-Z, and 20 printable ASCII symbols. Inclusion of all valid UTF-8 characters will further decrease the probability of a successful random guess.

[7] Sequential and repeating passwords consisting of digits 0-9 are not allowed. For example, the module will reject a password of 1-2-3-4-5-6-7 or 6-5-4-3-2-1-0. Attempts to create such a password will cause the module to indicate an error. There are 270 such combinations.

4 Physical Security

The multi-chip standalone cryptographic module includes the following physical security mechanisms, conforming to FIPS 140-2 Level 3 requirements:

1. Production grade components
2. Hard, opaque, tamper-evident enclosure with embedded, hard epoxy covering all security relevant components. Epoxy hardness was tested at ambient temperature and over the module's documented operating temperature range from 5 ˚C to 41 ˚C.
3. Memory protection enabled to prevent read-out of firmware, RAM, or NVRAM

The operator should periodically inspect the module for evidence of tampering.

5 Operational Environment

The FIPS 140-2 Operational Environment (Area 6) requirements for the module are not applicable because the device does not contain a modifiable operational environment.

6 Cryptographic Key Management

6.1 Cryptographic Algorithms

Algorithm	Modes	Key Sizes	Reference	CAVP Cert.	Use
AES	XTS[8]	256	NIST SP 800-38E[9]	4642	Encryption of user data within storage application only
AES	ECB CMAC CTR	128 256 (ECB only)	FIPS 197[10] NIST SP 800-38A[11]	5366	Block cipher basis of CTR-DRBG. Algorithmic basis of SIV.
AES	ECB GCM	128	FIPS 197 NIST SP 800-38A NIST SP 800-38D[12]	5397	AES-ECB is the block cipher basis for AES-GCM which is used to encrypt Bluetooth messages
CKG	-	256	NIST SP-800-133[13]	Vendor Affirmed	The unmodified output of the DRBG is used for generating symmetric keys.
DRBG	AES-CTR	256	NIST SP 800-90A[14]	2077	Random number generator for encryption keys and salts
ECDSA	-	P-256	FIPS 186-4[15]	1428[16]	Key generation for SP 800-56Ar2 key agreement
HMAC	HMAC-SHA-1	160	FIPS 198-1[17]	3554	Algorithmic basis of PBKDFv2
KAS	ECC CDH	P-256	NIST SP 800-56Ar2[18]	Vendor Affirmed (CVL 1857)	Key agreement for securing Bluetooth messages using ECC CDH Primitive (CVL 1857) for sharing secret computation, ECDSA (1428) for key pair generation, and SHS (4308) for single-step key generation
KBKDF	AES-CMAC	128	NIST SP 800-108[19]	201	Derivation of keys for Bluetooth message encryption
PBKDFv2	HMAC-SHA-1	-	NIST SP 800-132[20]	Vendor Affirmed	KEK generation. Password is the same as the User/CO Password with a minimum length of 7 characters. Algorithm conforms to FIPS 140-2 Implementation Guidance (IG) D.6: the module supports option 2a as documented in SP 800-132 § 5.4.
SHS	SHA-1	-	FIPS 180-4[21]	4308	Algorithmic basis of HMAC-SHA1

Table 7: FIPS Approved Algorithms

[8] ECB and CBC modes as well as 128 bit AES are included in the CAVS certificate, but are used by no services in the module.

[9] *SP 800-38E – Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices*. NIST. (January 2010).

[10] *FIPS 197 – Advanced Encryption Standard (AES)*. NIST. (November 2001).

[11] *SP 800-38A – Recommendation for Block Cipher Modes of Operation: Methods and Techniques*. NIST. (December 2001).

[12] *SP 800-38D – Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*. NIST. (November 2007).

[13] *SP 800-133 – Recommendation for Cryptographic Key Generation*. NIST. (December 2012).

[14] *SP 800-90Ar1 – Recommendation for Random Number Generation Using Determinstic Random Bit Generators*. NIST. (June 2015).

[15] *FIPS 186-4 – Digital Signature Standard (DSS).* NIST. (July 2013).

[16] Certificate #1428 covers only key pair generation. Signature and verification functions are not used.

[17] *FIPS 198-1 – The Keyed-Hash Message Authentication Code (HMAC)*. NIST. (July 2008).

[18] *SP 800-56Ar2 – Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. NIST. (May 2013).

[19] *SP 800-108 – Recommendation for Key Derivation Using Pseudorandom Functions (Revised)*. NIST. (October 2009).

[20] *SP 800-132 – Recommendation for Password-Based Key Derivation: Part 1: Storage Applications*. NIST. (December 2010).

[21] *FIPS 180-4 – Secure Hash Standard (SHS)*. NIST. (August 2015).

Algorithm	Reference	Caveats	Use
NDRNG		Module generates cryptographic keys with a minimum security strength of 256 bits.	Entropy source for seed to CTR-DRBG

Table 8: FIPS Allowed Algorithms

6.2 Critical Security Parameters

The module does not input or output private or secret cryptographic keys. Cryptographic keys are established per SP 800-56Ar2 scheme C(0s,2e,ECC_CDH) and conforming to SP 800-133. KEKs are derived using PBKDFv2 and are only used as part of the module's data storage application. Public/private key pairs are ephemeral, used for one and only one key agreement, and destroyed immediately after use.

Parameter	Use	Source	Storage	Creation / Destruction
CTR-DRBG state (seed, V, key)	Generating random values for CSPs	NDRNG and CTR-DRBG	RAM	Created when DRBG is seeded which is every time the module initializes
				Destroyed on lock, connect, successful generation of CSPs, power-off, and zeroization
User Password	Input to PBKDFv2 to allow generation of the User KEK.	Keypad entry	RAM	Created by User
				Destroyed on lock, unlock, timeout, and power-off
CO Password	Input to PBKDFv2 to allow generation of the CO KEK.	Keypad Entry	RAM	Created by CO
				Destroyed on lock, unlock, timeout, and power-off
User Salt	Input to PBKDFv2 to generate key to wrap DEK.	CTR-DRBG	NVRAM	Created when User changes Password
				Destroyed on Password change, zeroization
CO Salt	Input to PBKDFv2 to generate key to wrap DEK.	CTR-DRBG	NVRAM	Created when CO changes Password
				Destroyed on Password change, zeroization
XTS-AES DEK	Encryption and decryption of user data	CTR-DRBG	RAM	Created when first password, either User or CO, is set
				Destroyed on lock, timeout, entering low-power mode, power-off, and zeroization
User KEK	Encryption (wrapping) and decryption (unwrapping) of DEK	User Password, User Salt, and PBKDFv2	RAM	Created before encrypting or decrypting the DEK.
				Destroyed immediately after use.
CO KEK	Encryption (wrapping) and decryption (unwrapping) of DEK	CO Password, CO Salt, and PBKDFv2	RAM	Created before encrypting or decrypting the DEK.
				Destroyed immediately after use.
ECC-CDH Private Key	Bluetooth Message Encryption	CTR-DRBG	RAM	Generated when Bluetooth client requests secure channel
				Destroyed when secure channel established
Session Master Secret	Bluetooth Message Encryption	ECC-CDH Key Agreement	RAM	Created when secure channel established
				Destroyed when secure channel session ends
AES-GCM Key / IV	Bluetooth Message Encryption	Session Master Secret and KDF-AES-CMAC	RAM	Created when secure channel established or when secure channel is rekeyed
				Destroyed when secure channel session ends

Table 9: Critical Security Parameters

Parameter	Use	Source	Storage	Creation / Destruction
ECC-CDH Public Key	Bluetooth Message Encryption	ECC Primitive	RAM	Generated when Bluetooth client requests secure channel
				Destroyed when secure channel established
ECC-CDH Peer Public Key	Bluetooth Message Encryption	Remote Bluetooth Client	RAM	Generated when Bluetooth client requests secure channel
				Destroyed when secure channel established

Table 10: Public Security Parameters

6.3 Zeroization of Critical Security Parameters

Zeroization is the erasure of CSPs from volatile and non-volatile storage. The module initiates an erase cycle to zeroize CSPs stored in NVRAM. Copies of CSPs in RAM are erased by setting the memory to zeros. This process occurs when the module is factory reset or when the module detects a brute-force attack.

There are two kinds of brute-force attacks. Ten consecutive failed attempts to unlock the module as the User is the first type of brute-force attack and will zeroize the User CSPs. After this type of attack, the CO will be able to unlock the module, recover user data, and permit the setup of a new User Password. However, if there is no CO Password, the user data partition will be erased leaving the module in the factory reset state with an erased use data partition.

The second kind of brute-force attack is against the CO Password. Ten consecutive failed attempts to unlock the module as CO will zeroize all CSPs for both the CO and User rôles, including the DEK. The module will be left in the factory reset state with an erased user data partition.

7 EMI/EMC Regulatory Compliance

This module conforms to the EMI/EMC requirements specified by Title 47 of the Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., for home use).

8 Self-Tests

When the module powers on, it performs initialization and runs a sequence of self-tests. If any of these tests fails, the drive will enter an error state. The module cannot perform any cryptographic services and is not usable in this state. The module also performs conditional self-tests. The only way to clear a module error state is to cycle the power. Self-tests are summarized in Table 11.

Test Category	Test Name	When Executed	Error Indication
Firmware Integrity	Firmware CRC-32	Module power-on	Module illuminates no LEDs and does not respond to button presses.
	Firmware CRC-16	Module power-on	Module fails to mount to host PC after successful unlock and returns to locked state.
Known Answer	DRBG Cert. #2077 KATs CTR-DRBG Instantiate CTR-DRBG Generate	Module power-on	LEDs illuminate in continuously circling pattern, red then green then blue.
	PBKDFv2 combined KAT[22] HMAC SHA-1 Cert. #3554 SHA-1 Cert. #4308	Module power-on	LEDs illuminate in continuously circling pattern, red then green then blue.
	SIV KATs AES ECB encrypt Cert. #5366 AES ECB decrypt Cert. #5366 AES CMAC Cert. #5366	Module power-on	LEDs illuminate in continuously circling pattern, red then green then blue.
	XTS-AES Cert. #4642 KATs AES-XTS encrypt AES-XTS decrypt	Module power-on	Module fails to mount to host PC after successful unlock.
	AES-GCM Cert. #5397 KATs AES-GCM authenticated encrypt AES-GCM authenticated decrypt	Module power-on	LEDs illuminate in continuously circling pattern, red then green then blue.
	SP 800-56Ar2 KAS KATs per IG 9.6 Primitive 'Z' Computation KAT CVL Cert. #1857 SHA-1 KDF KAT Cert. #4308 AES CMAC (KDF Prerequisite) KAT Cert. #5366	Module power-on	LEDs illuminate in continuously circling pattern, red then green then blue.
Conditional	ECC Pairwise Consistency; Key Generation per SP 800-56Ar2 §5.6.2.1.4 for ECDSA Cert. #1428	Use of SP 800-56Ar2 Key Agreement	LEDs illuminate in continuously circling pattern, red then green then blue.
	ECC Partial Public-Key Validation; Assurance per SP 800-56Ar2 §5.6.2.2.2	Use of SP 800-56Ar2 Key Agreement	LEDs illuminate in continuously circling pattern, red then green then blue.
	NDRNG Conditional Test	Use of NDRNG	LEDs illuminate in continuously circling pattern, red then green then blue.
	XTS-AES; Key validity per IG A.9 CAVP #4642	Creation of DEK	Module fails to mount to host PC after successful unlock.

Table 11: Module Self-Tests

[22] A single KAT for HMAC incorporates the SHA test.

9 Mitigation of Other Attacks

The module has not been designed to mitigate attacks not addressed by the security requirements of FIPS 140-2.

10 Glossary of Terms and Acronyms

Term	Definition
AES	Advanced Encryption Standard
AES-GCM	AES Galois Counter Mode cipher used to encrypt Bluetooth messages
CO	Cryptographic Officer
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
CTR-DRBG	Counter-Mode Deterministic Random Byte Generator
DEK	Data Encryption Key
DRBG	Deterministic Random Byte Generator
ECB	Electronic Code Book
ECC	Elliptical Curve Cryptography
ECC-CDH	ECC Cofactor Diffie Hellman
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Protocol
HMAC	Keyed-Hash Message Authentication Code
KAT	Known Answer Test
KDF	Key Derivation Function
KEK	Key Encryption Key
LED	Light Emitting Diode
NDRNG	Non-deterministic Random Number Generator; module entropy source
NIST	National Institute of Standards and Technology

NVRAM	Non-volatile Random Access Memory
PBKDFv2	Password Based Key Derivation Algorithm Version 2
Password	User's secret authentication character sequence
RAM	Random Access Memory
Salt	Random value used to improve security of cryptographic algorithms
SATA	Serial AT Attachment
SHA-1	Secure Hash Algorithm 1
SHS	Secure Hash Standard
SIV	Synthetic Initialization Vector
USB	Universal Serial Bus
XTS-AES	AES cipher mode used to encrypt user data in mass storage
Zeroization	The process of erasing cryptographic security keys and parameters